REVISTA Sinergia

USO DE LOS SISTEMAS INTELIGENTES PARA LA DETECCIÓN DE FRAUDES FINANCIEROS.

Fernando Gutiérrez-Portela
Estudiante Doctorado en Ingeniería de la Universidad Autónoma de Bucaramanga. Magíster en Software Libre, Profesor de Ingeniería de Sistemas e Ingeniería Civil de la Universidad Cooperativa de Colombia Sede Ibagué - Espinal. Integrante del Grupo de Investigación AQUA de la UCC Ibagué – Espinal.
Correo: fernando.gutierrez@ucc.edu.co

John Johver Moreno-Hernández
Doctorando en Administración de la Universidad Externado de Colombia. Profesor de la Universidad Cooperativa de Colombia sede Ibagué – Espinal.
Correo. john.morenoh@campusucc.edu.co

Brillid Dayhanna Echeverry
Estudiante de la Universidad Cooperativa de Colombia Programa de Contaduría Pública Sede Ibagué – Espinal.
Correo brillid.echeverryc@campusucc.edu.co.

Anderson Estiven Jaramillo
Estudiante de la Universidad Cooperativa de Colombia Programa de Contaduría Pública Sede Ibagué – Espinal.
Correo anderson.jaramillos@campusucc.edu.co

Enviado: 20 de agosto de 2019
Aceptado: 20 septiembre de 2019
Publicado: 28 diciembre de 2019

INSTITUCIÓN UNIVERSITARIA COLEGIO MAYOR DE ANTIOQUIA
Alcaldía de Medellín Cuenta con vos SAPIENCIA Agencia de Educación Superior de Medellín

USO DE LOS SISTEMAS INTELIGENTES PARA LA DETECCIÓN DE FRAUDES FINANCIEROS.

Resumen

En el mundo, los fraudes financieros han presentado un grave problema para las organizaciones, ocasionados en su mayoría, por falta de controles. A su vez, los avances tecnológicos han abierto puertas para llevar a cabo fraudes que son difíciles de detectar a tiempo. Es así, que a partir de la creación de núcleos de procesamiento tecnológico se ha podido detectar patrones que permiten alertas respecto a fraudes o acciones de nivel sospecho.

Por lo anterior, el objeto de este artículo es analizar estudios de casos de aprendizaje de máquina *(Machine Learning*) usados en fraudes financieros. Metodológicamente se inicia con una revisión en detalle del uso del aprendizaje automático en diferentes áreas, para luego analizar directamente la información en el área financiera. Se concluye afirmando que los sistemas inteligentes mejoran la efectividad en la detección de fraudes financieros.

PALABRAS CLAVE: Sistemas inteligentes, *Machine Learning*, fraudes financieros.

USE OF INTELLIGENT SYSTEMS FOR THE DETECTION OF FINANCIAL FRAUDS.

Abstract

In the world, financial frauds have presented a serious problem for organizations, mostly caused by lack of controls and, in turn, technological advances have opened doors to carry out frauds that are difficult to detect in time. Thus, since the creation of technology processing cores, patterns that suggest fraud or suspicious actions have been detected.

Therefore, the purpose of this article is the analysis of case studies of Machine Learning used in financial fraud. Methodologically it begins with a detailed review of the use of Machine Learning in different areas, and then directly analyzes the information in the financial area. It is concluded that intelligent systems help detect financial fraud.

Keywords: *Intelligent Systems, Machine Learning, Financial Fraud.*

INTRODUCCIÓN

El fraude financiero desde la apertura económica de 1980 ha tomado espacios de análisis en su detección temprana, no solo de las entidades bancarias, sino en administradores, académicos, ingenieros de sistemas, entre muchos otros. En las últimas décadas se han creado núcleos de procesamiento complejo para la detención de anomalías financieras, permitiendo vincular la inteligencia artificial con procesos de detección de fraudes.

En este sentido, existen técnicas de datos para la detención de patrones anómalos a través del uso de sistemas inteligentes que aprenden de manera constante, para reaccionar sobre situaciones que son consideradas "de alerta" y así determinar de forma temprana un suceso próximo a presentarse.

Teniendo como objetivo general el analizar los estudios de caso que utilizan sistemas inteligentes (*Machine Learning* –ML–) bajo el estándar de algoritmos determinísticos, a través de la caracterización de los sistemas inteligentes usados en los casos de estudios para la detección de fraudes financieros no supervisados, relacionando las variables que se tuvo en cuenta para construcción de este sistema inteligente

Se realiza bajo una revisión empírica de estudios de caso, con una metodología de naturaleza cualitativa descriptiva, lo que lleva a unas conclusiones que servirán de referente al lector interesado. Este estudio se plantea en cuatro apartados: en el primero se registra un marco teórico, luego se analizan los estudios de casos de

fraudes financieros no supervisados, en tercer lugar, se analizan las variables con las que se construyeron los sistemas inteligentes, y finalmente se realiza una relación de auditorías que se pueden tener con estos sistemas inteligentes, y por último las conclusiones y Bibliografía.

MARCO TEÓRICO

Machine Learning

La globalización y la inclusión financiera desde 1980 generó que aparecieran las primeras transacciones virtuales con tarjetas de crédito, lo que ha permitido el desarrollo de fraudes financieros que se han fortalecido en mayor medida a través del tiempo, requiriéndose la utilización de modelos de técnicas de inteligencia artificial bajo el estándar de algoritmos determinísticos para la mutación del comportamiento fraudulento.

Siendo importante resaltar que las entidades financieras requieren detectar de manera temprana los fraudes a partir de transacciones de crédito y débito, por lo que el modelo de técnicas de inteligencia a partir de algoritmos determinísticos se los ha permitido.

El aprendizaje de máquina (*Machine Learning*), como se denomina en inglés, se refiere al estudio de algoritmos de computadora que mejoran automáticamente a través de la experiencia. Este tipo de aprendizaje se ha utilizado en aplicaciones que van desde la minería de datos que descubren las reglas en grandes conjuntos

de datos hasta sistemas de filtración de información que automáticamente aprenden los intereses de los usuarios (Calvo Valverde, 2016).

De igual manera, los algoritmos de ML se utilizan para la identificación de páginas web maliciosas a partir de la extracción de información de análisis estático y dinámico como lo indicó (Navarro & García, 2017), quien argumenta que investigaciones como las de Mohaisen en el 2015 donde se entrenaron y testearon clasificados a través de la información obtenida de objetos transferidos (TF) en el tráfico HTTP tanto de páginas malignas y benignas, con un resultado de detección de 93 % en páginas web maliciosas.

Por último, Calvo Valverde (2016) , toma como referente la postura de Murphy 2012 quien relacionó el aprendizaje de máquina como un conjunto de métodos que automáticamente pueden detectar patrones en los datos y usar los patrones descubiertos para predecir datos futuros o para ejecutar otra clase de toma de decisión bajo incertidumbre, como, por ejemplo, planificar cómo recolectar más datos.

Machine Learning para fraudes financieros

Las técnicas de aprendizaje se utilizan para la detención de fraude en pagos con tarjeta en el campo de anomaly/outlier detection, como fuentes de datos que alimentan los sistemas, a partir de tecnologías de colas de mensajes como TIBCO EMS y Kafka.

Por lo tanto, los datos generados en una transacción son enviados a estas colas para que los respectivos sistemas puedan procesarlos y aplicar el algoritmo de aprendizaje máquina, determinando si una nueva instancia es fraude o no. Ambos sistemas hacen uso de una base de datos MongoDB para almacenar los datos generados de forma pseudoaleatoria por los generadores de mensajes, correspondientes a movimientos de tarjetas. Estos movimientos posteriormente son usados como conjunto de entrenamiento para el algoritmo de aprendizaje máquinas (Montero, 2016).

Sistemas de Detención Supervisado y No Supervisado

Morales (2018) señala que, la principal finalidad de un sistema de detección de intrusos (IDS) es monitorear la actividad en un servidor o en una red, de tal manera que se puedan obtener pistas y alertas de posibles ataques o intentos de violación a la seguridad. Es así que, un IDS identifica actividad «no deseada», genera alarmas y utiliza mecanismos de detección de estos eventos no deseados, los cuales están basados normalmente en patrones de comportamiento, firmas de código o análisis de protocolos. Pero estos no son perfectos y pueden presentarse comportamientos fallidos del sistema

Ahora bien, el sistema de detección de fraudes supervisado, se realiza a partir de la alerta del IDS en el sistema dando aviso a un operador, quien inicia la respectiva vigilancia, determinando la respuesta que debería generar la red a partir de una entrada determinada. El supervisor comprueba la salida generada por el

sistema y en el caso en que no coincida con la esperada, procederá a modificar los pesos de las conexiones y/o su arquitectura, con el objetivo de refinar y mejorar las predicciones del modelo. Este proceso se repite hasta alcanzar la configuración óptima (Cardenas, s,f).

Weber (2000) indicó sobre la detención supervisada y no supervisada y una relación de ejemplos como el de los paradigmas de aprendizaje supervisado, la red se enfoca en un conjunto de entrenamiento representativo que consiste en pares vectoriales. Uno de los vectores se aplica a la entrada de la red, el otro se usa de objetivo, representativo de la salida deseada. El entrenamiento se logra al ajustar los pesos de las conexiones de la red para minimizar la diferencia entre las salidas deseadas y las salidas computadas. El aprendizaje no supervisado, muchas veces llamado auto-organización, solamente requiere de vectores de entrada para adiestrar la red. Durante el proceso de entrenamiento, las ponderaciones de la red se ajustan a fin de que las entradas similares produzcan salidas similares. Esto se logra mediante el algoritmo de entrenamiento que extrae regularidades estadísticas desde el conjunto de entrenamiento.

Caballero (2017), manifestó como otro paradigma de aprendizaje el semi-supervisado con el que se pueden solucionar problemas que de una u otra manera no pertenecen de forma exacta a ninguna clase y mediante técnicas probalísticas o haciendo uso de clasificadores específicos se solventa el problema.

Ahora bien, con estos sistemas de detención supervisado y no supervisado, se han localizado algunos tipos de fraudes como el fraude bancario, el fraude de

seguros, el fraude de marketing en internet y el fraude en las telecomunicaciones. Si bien, en cada uno de ellos se puede relacionar técnicas ilícitas que a continuación se relacionaran algunas.

- Dentro del fraude bancario se identifican técnicas como el *Phishing*; en este sentido, la Coltefinanciera (2014), determinó este fraude como «una técnica de captación ilícita de datos personales y de cuentas bancarias y la utilizan para abrir otras cuentas a nombre del usuario». De otro lado, está el fraude de las tarjetas, en donde la técnica de *Skimming* con la copia de la información de la banda magnética de la tarjeta original que ha sido tomada antes de ser entregada al titular.
- En cuanto al fraude en los seguros se analizan que dentro sus modalidades están seguros médicos, de automóvil, hogar y cosecha se han detectado técnicas avanzadas por medios electrónicos.

Caballero (2017) caracterizó doce tipos de fraude así, como son fraude de tarjeta de crédito, defraudar al seguro, la corrupción en los diferentes niveles de poder, la falsificación, fraude en la garantía de un producto, fraude sanitario, fraude en las telecomunicaciones, el de lavado de dinero -en el que se obtienen beneficios por actividades ilegales y hacer que parezcan legales-, fraude del click, con el que se benefician a través de la acción repetidas veces para autoincrementar ganancias en un anuncio o página web, fraude a través del robo de identidad, y por último el plagio.

MATERIALES Y MÉTODOS

La realización de este artículo partió de una revisión documental empírica y teórica, tomando como estudio casos relevantes, donde se usan los sistemas inteligencias para la detención de fraudes, la información fue recopilada a través de bases de datos de reconocidos con los que se pudo tomar lo más relevante para cada objetivo propuesto. El corte temporal definido para esta revisión documental fue durante el 2019, lo que permitió llegar a unas conclusiones

RESULTADOS

Sistemas Inteligentes para fraudes financieros no supervisados

Al caracterizar los sistemas inteligentes usados en los casos de estudios para la detección de fraudes financieros no supervisados se encontró relevante un estudio, que tomó las tecnologías de TIBCO herramientas comerciales diseñadas para eventos complejos y Apache Spark, un sistema abierto para el procesamiento de datos en tiempo real los comparo y analizó, aplicando técnicas de aprendizaje máquina, concretamente del campo de anomaly/outlier detection (Montero, 2016).

Tabla 1. *Tecnologías de TIBCO- herramientas comerciales diseñadas para eventos complejos y Apache Spark.*

Autores	Antecedentes	Fraudes	Solución	
Montero (2016)	TIBCO y Apache Spark. Ambas tecnologías son muy utilizadas en el mundo actual, y cada una de ellas afronta un paradigma de programación distinto, procesamiento de eventos complejos en el caso de TIBCO, y procesamiento en tiempo real en el caso de Spark Streaming	Fraude en pagos con tarjeta de crédito en tiempo real	Se creó un sistema de tecnología de procesamiento distribuido.	Se consideran dos tipos de tecnologías: TIBCO y APACHE SPARK. con el objeto de incrementar la difusión, uso e impacto del trabajo en internet y garantizar su preservación y acceso a largo plazo

Fuente: Montero (2016) adaptada por los autores.

De igual forma, se analiza que se usaron tecnologías de colas de mensajes como *TIBCO EMS y Kafka*, aplicando el algoritmo de aprendizaje máquina, determinando si una nueva instancia es fraude o no. Se tuvo en cuenta variables de proceso como; *Element of Type*: esta opción permite establecer tipos básicos, *String, Decimal, Boolean, Integer, Date, Binary, URI. XML Reference*: esta opción hace referencia un recurso de tipo Schema que define la estructura de un *XML*.

Para diseñar el detector de fraude en tiempo real se realizaron cuatro fases así: a) fase de generación de movimientos, b) fase de filtro de mensajes, c) fase de consultas en base de datos, y d) fase de detención de anomalías, donde se evidenció que después de terminar la investigación, su experiencia ha sido exitosa ya que hoy día tiene muchos usos en la predicción de tasas, y enfermedades, pero debe ampliar el conocimiento en base de datos noSQL ya que actualmente es muy utilizada.

Tabla 2. *Programación genética para detección de fraudes financieros*

Autores	Antecedentes	Fraudes	Solución
(Coello, 2010)	Walker et al. reportan el uso de programación genética para generar Fórmulas que mapeen valores observados en salidas esperadas. Visa International tiene actualmente en operación en sistema de detección de fraudes que usa redes neuronales, el cual ha sido empleado por 5 bancos canadienses y 10 bancos norteamericanos, cubriendo a unos 40 millones de tarjetahabientes	financiero financiero	Evaluación estadística. Detectar actividades Fraudulentas, comparando transacciones legales con casos previos de fraude. Una vez que la red ha aprendido ciertos patrones de comportamiento "sospechosos", se le utiliza para alertar a un experto humano cuando una cierta transacción pudiese Resultar fraudulenta.

Nota: *Sistemas de detección de fraudes financieros a través de redes neuronales*.
Fuente: Coello (2010)

Coello (2010), realizó una demarcación de soluciones a problemas financieros de diversa índole, entre ellos asignaciones de créditos y riesgos en préstamos hipotecarios. De igual manera, hace un barrido frente a otra clase de riesgos como de seguros y de mercadotecnia, inversiones, vigilancia, planeación, resaltando el cubrimiento y detención que permiten los sistemas inteligentes.

Tabla 3. *Detección de fraudes en datos contables.*

Autores	Antecedentes	Fraudes	Solución
(Perez, 2015)	Ley de Benfor Análisis de Regresión y correlación. Análisis de frecuencia digital. Análisis histórico de tendencias.	En datos contables	Detención números anómalos.

Fuente: Perez (2015) Adaptada por los autores

Nota: Señales de alerta frente a movimientos anomalos a traves de análisis de regresión y correlación, análisis de frecuencia digital y análisis histórico de tendencias.

En este estudio (Perez, 2015), se clarifica que estos tipos de sistemas inteligentes no identifican claramente que hay un fraude, solo demuestra o da señales de alerta frente a movimientos anómalos.

Variables de para la construcción de un sistema inteligente

Los computadores son capaces de ejecutar manipulaciones numéricas y simbólicas de formas rápidas y eficientes tal y como sucede con el manejo de grandes bases de información y con la implementación de modelos matemáticos en el computador que tratan de reproducir comportamiento de fenómenos, procesos que tienen lugar en la naturaleza entre otros, por lo que para la construcción de un sistema inteligente el conocimiento es explícitamente expresado en palabras y símbolos, y las aproximaciones numéricas tales como las redes neuronales artificiales, los algoritmos genéticos y la lógica difusa (Obregon & Fragala, 2012).

Tabla 4. *Caracterización de los sistemas inteligentes en los estudios de caso*

Sistemas inteligentes	Logaritmo	Lenguaje de programación		
Tecnología Inteligente PS Fraud	WSDL	Lenguaje de protocolos.	Reduce significativamente las alertas falsas	Logra anticiparse al fraude logrando incrementar el saldo disponible salvado, a la vez que minimiza la posibilidad de ocurrencia de fraudes posteriores, así mejorando la detección del fraude bancario, financiero, electrónico u otras variaciones de fraude que se puedan presentar en la entidad, según su naturaleza.

Fuente: Predisoft (2018)

Nota: *Tecnología inteligente para la detección de fraudes bancarios, financieros, electrónicos u otros*.

Por otra parte, se (Nur-E-Arefin, 2010) realizó un estudio sobre técnicas de detección de fraude en tiempo real, utilizando diferentes algoritmos de clasificación de minería de datos. Lo denominó aplicación de inteligencia computacional para identificar fraudes con tarjetas de crédito.

Tabla 5. *Técnicas de detección de fraude en tiempo real*

Autores	Antecedentes	Fraudes	Solución
(Nur-E-Arefin, 2010)	Inteligencia Artificial Aplicada Redes Neuronales Clasificador Bayesiano Detención de valores atípicos Mapas auto-organizados Máquinas de vectores de soporte sistema neuro-difuso Algoritmo genético Detención Table DTNB – Tabla de detención clasificadora.	Transacciones anómalas en tarjetas de crédito.	Clasificador para detectar fraude en Línea. (Titular no está presente) Robo/Fraude de Aplicaciones/Falsificación de Tarjetas/Emisiones no Recibidas

Fuente: Nur-E-Arefin (2010)

Nota*: Uso de algoritmos de clasificación de minería de datos para la detección de fraudes en tiempo real.*

Tabla 6. *Caracterización del sistema, concurso de minería de datos de uc*

Sistemas inteligentes	Logaritmo	Lenguaje de programación		
Concurso de Minería de Datos de UC	WEKA,DTNB-X1,Decision Table, OneR, Bayes Net, NaiveBayes, Ibk, Ib1,Kstar, Lwl, Bagging, Dagging, END, Multiclassclassifer,Classification ViaRegression,LMT y J48	Lenguaje de protocolos.	Detección transacciones anómalas en línea de tarjeta crédito.	Se realiza la prueba del tren donde el conjunto de datos se distribuye en un 66% y un 34% en precisión de clasificadores. Se utiliza La validación cruzada

Fuente: (Universidad Central , 2017)

Nota: Uso de lenguaje de protocolos para la detección de transacciones anómalas en línea de tarjeta de crédito

Jeragh & AlSulaimi (2008), presenta un análisis sobre la combinación de codificadores automáticos y una máquina de vectores de soporte de clase para la detección de transacciones fraudulentas de tarjetas de crédito. Presenta un modelo de aprendizaje no supervisado basado en la combinación de un codificador automático y una máquina de vectores de soporte de una clase (OSVM).

Tabla 7. Detección de transacciones fraudulentas de tarjetas de crédito.

Autores	Antecedentes	Fraudes	Solución
(Jeragh & AlSulaimi, 2008)	redes neuronales Árboles de decisión (DT). aprendizaje automático no supervisado	fraude con tarjetas de Crédito.	una entrada se alimenta a un codificador Automático y se produce un error de reconstrucción de entrada - se pasa a un OSVM para determinar si una transacción es fraudulenta.

Fuente. Jeragh & AlSulaimi (2008).

Nota: Usos de combinación de codificadores automáticos y una máquina de vectores de soporte de una clase para la detección de transacciones fraudulentas de tarjetas de crédito.

Tabla 8. *Caracterización del sistema hiperplano e de OSVM máquina de vectores de soporte.*

Sistemas inteligentes	Logaritmo	Lenguaje de programación	
hiperplano e de OSVM máquina de vectores de soporte	MSE (distancia medida por el error cuadrático medio)	TensorFlow, biblioteca de aprendizaje profundo. Scikit Learn, biblioteca de aprendizaje automático.	Combinación de codificadores Automáticos profundos y OSVM. un modelo de aprendizaje automático no supervisado se entrena en una sola clase(una transacción regular o genuina) y que después de la capacitación Distingue entre transacciones genuinas y fraudulentas.

Fuente: Berrendero (2015)

Nota: Codificadores automáticos y OSVM.

En este documento, se presenta un modelo sin supervisión basado en la combinación de codificadores automáticos y OSVM. La combinación permite inferir relaciones y dependencias ocultas entre las características de la entrada.

Tabla 9. *Análisis sobre la detección de fraudes con tarjeta de crédito.*

Autores	Antecedentes	Fraudes	Solución
(Sharmila; et al, 2010)	algoritmo genético Árbol de decisión Algoritmo de anomalía basado en LOIF Algoritmo para la Detección de Anomalías como Algoritmo de bosque de aislamiento (IFA) diagrama de matriz de correlación.	Transacciones fraudulentas con tarjeta de crédito.	Visualización de datos para mostrar el resultado de formas más comprensibles que incluyen histogramas, gráficos y matriz. con la ayuda de técnicas de visualización de datos se detectan las transacciones fraudulentas de la correcta.

Fuente: Sharmila; et al (2010)

Nota: Análisis denominado Credit Card Fraud Detection Using Anomaly Techniques para la deteccion de frauds con tarjeta de crédito.

De igual foma, Rahul, Seth, & Kumar (2018), realizaron un estudio sobre la detención de manipulación de ganancias y el fraude contable que relacionaron como detección de manipulación de ganancias:

Tabla 10.

Uso del aprendizaje automático para la detección de fraudes financieros.

Autores	Antecedentes	Fraudes	Solución
(Rahul, Seth, & Kumar, 2018)	Modelo Healy, modelo DeAngelo, modelo Jones, modelo industrial PCGA principios de contabilidad generalmente aceptados CEO comportamiento de manipulación de las ganancias	Detecta la manipulación acumulativa de datos.	Identifica y compara los Modelos de conjuntos existentes que establecen la superioridad de datos.

Fuente: Rahul, Seth, & Kumar (2018)

Nota: Detección de la manipulación acumulativa de datos.

Con los avances tecnológicos de la actualidad, la manipulación acumulativa de datos se puede detectar o predecir antes de que el fraude sea cometido, existen algunas plataformas financieras que realizan esto como lo son Falcon Fraud manager y sas fraud management las cuales utilizan análisis de datos de aprendizaje automático por un procesamiento analítico esencial deinteligencia artifcial para gestionar las necesidades de detección de fraude transaccional y monitoreo en pagos en una organización (Gonzalez, Romero, & Ortiz, 2018).

Tabla 11. *Modelos de conjunto supervisados y no supervisados de aprendizaje automático.*

Sistemas inteligentes	Logaritmo	Lenguaje de programación	
Modelos de conjunto supervisados y no supervisados de aprendizaje automático	ROC (métrica de rendimiento para conjuntos de datos desequilibrados)	logit / probit	Teoría del préstamo del trabajo seminal Realizado por Beneish. Técnica de muestreo basada en simulación para manejar eficientemente el conjunto de datos desequilibrados e ilustrar resultados en datos de empresas que cotizan en la bolsa.

Fuente. (Fuentes, 2018)

Nota: Uso del logaritmo ROC (métrica de rendimiento para conjuntos de datos desequilibrados).

Kumar & Iqbal (2017), establecieron un estudio sobre técnicas de detección de fraudes de MasterCard que denominaron Identificación de fraude con tarjeta de crédito utilizando Enfoques de aprendizaje automático.

Tabla 12. *Técnicas de detección de fraudes de MasterCard*

Autores	Antecedentes	Fraudes	Solución
(Kumar & Iqbal, 2017)	Red neuronal (NN), Técnicas de inducción de reglas, Sistema difuso, Arboles de llamadas, Máquinas de vectores de soporte (SVM), Regresión logística, Factor local atípico (LOF), Bosque de aislamiento, vecino K Más cercano, Algoritmos genéticos.	Fraudes En línea o fraudes con tarjetas de crédito.	Clasifica. varias técnicas utilizadas en la detección de fraudes de MasterCard y evalúa cada criterio vinculado con metodología admitida localiza patrones legales y criminales de transacciones que manejan el desequilibrio

Fuente: Kumar & Iqbal (2017)

Nota: Técnicas de detección de fraudes en línea de tarjetas de crédito.

Se lanza un sistema de detección de fraudes MasterCard ayudar a los bancos a combatir el fraude. Se trata del sistema de detección temprana. Esta herramienta le ofrece a los bancos emisores una alerta avanzada única para tarjetas y cuentas que tienen un riesgo elevado de uso fraudulento, debido a su exposición a incidentes de seguridad anteriores o filtraciones de datos, El sistema puede identificar la comercialización activa de datos de cuentas y tarjetas (Angulo, 2017).

Tabla 13. *Caracterización del sistema de detección de fraudes de Master Card*

Sistemas inteligentes	Logaritmo	Lenguaje de programación	
Minería de valores atípicos. estudios especializados de Dominio. Aprendizajes supervisados y no supervisados	MLP / emplea algoritmos de Aprendizaje automático. KNN, Random Forest, SVM y Naïve Bayes. La técnica Clave proyectada es "Fraud Miner".	Localhost	obtienen Resultados mediante el uso de datos normalizados.

Fuente: Kumar & Iqbal (2017)
Nota. Caracterización del sistema a través de la minería de valores atípicos.

Relación de auditorías que se pueden tener con estos sistemas inteligentes

La auditoría de bases de datos consiste en un proceso de monitoreo continuo de los controles que la administración ha establecido dentro de los sistemas de sus bases de datos, y todos sus componentes, para obtener una seguridad razonable de la utilización adecuada de los datos que son almacenados por los usuarios mediante los sistemas de información. El monitoreo y pruebas a los controles determinan la pertinencia y suficiencia de éstos, permitiendo entonces ajustar, eliminar o implementar nuevos controles para asegurar su adecuada utilización (Murillo, 2008).

Con los sistemas inteligentes se da paso a auditorías internas y externas, dentro de ellas se encuentra el sistema de información contable, la responsabilidad ética e independencia, llevando a los bancos con rapidez, eficiencia y eficacia información para la toma de decisiones y acercándolos con los órganos de control, a un marco de auditoria estratégica, de gobernabilidad y de talento humano, mostrando con ello factores importantes como resiliencia cibernética, calidad de datos, infraestructura de datos, niveles de desempeño y algo relevante la ética.

Todos estos controles crean una serie de procesos de observación, generando instrucciones que habilitan actividades tanto internas como externas, dejando claro que hay algunos registros que no permite involucrar y conocer la intensión hasta después de que se genera un fraude.

Lo que sí es claro, es que con el uso de la inteligencia artificial se genera en alertas tempranas que se convierten en instrucciones que recibe el sistema otorgando a los clientes privilegios o permisos para la realización de consultas o realización de transacciones (Coltefinanciera, 2014).

CONCLUSIONES

Al analizar los estudios de caso que utilizan sistemas inteligentes (*Machine Learning*) para la detección de fraudes financieros, se determina que las técnicas de aprendizaje en la detención de fraudes o anomalías aplican algoritmos, teniendo en cuenta variables de procesos en tiempo real. Por otro lado, se evidencia que los sistemas inteligentes financieros han avanzado a nivel de la globalización, lo que ha

facultado la utilización de los procesos automáticos, que han avanzado en esferas de salud, entretenimiento, agronomía y gastronomía; pero que, a su vez, han sido usados en la detección temprana de anomalías financieras que afectan las finanzas de la organización

Al caracterizar los sistemas inteligentes mediante estudio de caso, se establece que se detecta actividades fraudulentas, una vez ha tomado patrones de comportamiento en objetos y actividades sospechosas y es allí donde radica la importancia del uso de sistemas inteligentes en fraudes financieros de forma supervisada, no supervisada y semi-supervisada, durante el proceso, ajustándose a similitudes mediante algoritmos de entrenamiento

En las variables que tuvieron en cuenta los casos objeto de estudio se señala el lenguaje de protocolos, el cual reduce las alertas falsas y se anticipa al fraude a través del uso de distintas combinaciones de algoritmos, análisis de regresión, procesamientos en tiempo real, redes neuronales entre otras.

Al evidenciar auditorías basadas en ML se señalan las internas y externas como la auditoría de seguridad, auditoría de seguridad física, auditoría de bases de datos, auditoria de seguridad lógica de la información, auditoría de seguridad de procesos, auditoría de la gestión de la información, auditoría a los datos y su protección, a través de procesos de observación que no permiten conocer la intensión hasta después de generado el fraude, ya que los estatutos o instructores solo otorga permisos de acuerdo a niveles de seguridad.

REFERENCIAS

Angulo, s. (17 de octubre de 2017). *Herramienta de mastercad*. Obtenido de https://www.enter.co/especiales/empresas/herramienta-mastercard-identifica-fraudes/

Berrendero, j. (13 de Febrero de 2015). *hiperplano e de OSVM*. Obtenido de Universidad autonoma de madrid: http://verso.mat.uam.es/~joser.berrendero/cursos/Matematicas-IO/io-tema6-svm-16.pdf

Caballero, L. (Julio de 2017). *Detención de sucesos raros con Machine Leaning*. Obtenido de file:///D:/Documents/Nueva%20carpeta/casas%20de%20justicia%20y%20juez%20de%20paz%20en%20equidad/tesis%20TFM_ANDER_CARRENO_LOPEZ.pdf

Calvo Valverde, L. A. (mayo de 2016). Estrategia basada en el aprendizaje de máquina para tratar con conjuntos de datos no etiquetados usando conjuntos aproximados y/o ganancia de información. *Scielo*, 4-15. Obtenido de https://www.scielo.sa.cr/pdf/tem/v29s2/0379-3982-tem-29-s2-4.pdf

Cardenas. (s,f). Modelos de Aprendizaje Supervisados: aplicaciones para la predicción de. *Sedini*, 1-5. Obtenido de http://sedici.unlp.edu.ar/bitstream/handle/10915/45467/Documento_completo.pdf?sequence=1&isAllowed=y

Coello, C. C. (2010). Uso de T閨nicas de Inteligencia Artificial Para Aplicaciones Financieras. 1-7.

Coltefinanciera. (17 de 12 de 2014). *Educación financiera*. Obtenido de https://www.coltefinanciera.com.co/educacion-financiera/fraudes-bancarios/398-modalidades-de-fraudes-bancarios-en-internet

Fuentes, A. (2 de Mayo de 2018). *Tipos de aprendizaje automatico*. Obtenido de Aprendizaje supervisado y no supervisado: http://machinelearningparatodos.com/tipos-de-aprendizaje-automatico/

Gonzalez, E., Romero, G., & Ortiz, A. (12 de junio de 2018). *Detección de Fraude en Tarjetas de Crédito.* Obtenido de Universidad santo tomas: https://repository.usta.edu.co/bitstream/handle/11634/12529/2018edwingonzalez.pdf?sequence=1&isAllowed=y

Jeragh, M., & AlSulaimi, M. (2008). Combinación de codificadores automáticos y una máquina devectores de soporte de clase para la detección de transaccionesfraudulentas de tarjetas de crédito. *UNAB*, 1-14.

Kumar, P., & Iqbal, F. (2017). Identificación de fraude con tarjeta de crédito utilizando enfoques de aprendizaje automático. *UNAB*, 1-9.

Montero. (12 de junio de 2016). *Detección de fraude bancario en tiempo real utilizando tecnologías de procesamiento distribuido*. Obtenido de https://eprints.ucm.es/38647/1/Memoria%20TFM%20Detecci%C3%B3n%20Fraude_FINAL.pdf

Morales, C. (2018). Modelo de Detección de Intrusos Usando Técnicas De Aprendizaje. 1-31. Obtenido de http://190.217.58.250/bitstream/tda/442/1/MODELO%20DE%20DETECCION%20DE%20INTRUSOS%20USANDO%20TECNICAS%20DE%20APRENDIZAJE.pdf

Murillo, J. V. (2008). Auditando En Las Bases de Datos. *Uniciencia 22*, 135-140. Obtenido de file:///D:/Downloads/Dialnet-AuditandoEnLasBasesDeDatos-5381374.pdf

Navarro, U., & García, C. (2017). Machine Learning Classifiers to Detect Malicious. *researchgate*, 1-4. doi:https://www.researchgate.net/profile/Christian_Urcuqui_Lopez/publication/320290759_Machine_Learning_Classifiers_to_Detect_Malicious_Websites/links/59e18b01458515393d53562e/Machine-Learning-Classifiers-to-Detect-Malicious-Websites.pdf

Nur-E-Arefin. (2010). Aplicacion de Inteligencia Computacional Para Identificar Fraudes con Tarjetas de Credito. *Universidad Autonoma de Bucaramanga*, 1-10.

Obregon, N., & Fragala, F. (2012). Sistemas inteligentes, ingenieria e hidroinformatica. *Ciencia e ingenieria Neogranadina*, 71-79.

Parada, M. A. (2012). Utilización de metodologías de Inteligencia Artificial y sus aplicaciones en El Salvador. *ING-NOVACIÓN*, 57-68. Obtenido de http://201.131.110.78/jspui/bitstream/10972/1950/1/7.%20Utilizacion%20de%20metodologias%20de%20Inteligencia%20Artificial%20y%20sus%20aplicaciones%20en%20El%20Salvador.pdf

Perez, L. (2015). prevencion de fraudes a traves del uso de las tecnologias. http://repositorio.unan.edu.ni/9650/1/17534.pdf.

Predisoft. (14 de Octubre de 2018). *Deteccion del fraude* . Obtenido de Sistema para la prevencion del fraude en multiples canales : http://predisoft.com/psfraud-sistema-deteccion-fraudes-bancarios-y-otros-canales/

Rahul, K., Seth, N., & Kumar, U. D. (2018). Detección de manipulación de ganancias:uso del aprendizaje automático para ladetección de fraudes financieros. *Springer Link*, 5-29.

Sharmila; et al. (2010). Credit Card Fraud Detection Using Anomaly Techniques. *UNAB*, 1-14.

Universidad Central . (24 de Octubre de 2017). *Deteccion de fraudes financieros* . Obtenido de https://www.ucentral.edu.co/en/noticentral/fernando-bomba-finalista-convocatoria-datos-u

Weber, R. (2000). Data Mining en la Empresa y en las Finanzas Utilizando Tecnologías Inteligentes. *Ingenieria de Sistemas*, 61-78. Obtenido de https://s3.amazonaws.com/academia.edu.documents/30817710/Vol14.pdf?response-content-disposition=inline%3B%20filename%3DData_Mining_en_la_empresa_y_en_las_finan.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWOWYYGZ2Y53UL3A%2F20190724%2Fus-east